Small businesses are commonly under the misconception that cybersecurity is only for larger organizations, since cyber criminals will only be interested in targeting them. This is not entirely true. The truth is that small and medium businesses are easier targets for cybercriminals, and thus they often suffer from security breaches as a result of their weak security practices. Therefore, it’s equally important for small businesses to take security measures.

However, it’s understandable that small businesses do not have enough investments to put into cybersecurity and they prioritize other business operations such as marketing. However, every business in today’s times depends on the internet in some way, and it’s not possible to ignore the importance of adopting safe cyber practices.

This does not mean that you need to necessarily invest a large amount. Even with a low budget, small business can focus on the basic but most important security practices to avoid potential breaches. Let’s look at some of the practices for small and medium businesses to ensure cybersecurity within the organization.

1. **Create Cybersecurity Policies**

Drafting security policies does not require investment. It needs you to be knowledgeable and understand how to comply with security frameworks and standards. For ensuring that your policies are properly documented and regulated in the organization, thoroughly draft them along with schedules and checklists to enforce their implementation.

1. **Back up Your Data**

With ransomware attacks on the rise, it is very important to keep a backup of your data, preferably in the cloud. This way, you can avoid paying huge ransom amount or recovery costs as your original data will be intact. It can also avoid downtimes.

For small businesses, cloud services are good backup sources. They not only allow one to access data from any location, but also let you provide considerable security.

1. **Review Access Controls**

One of the most important steps to ensure security is to implement access controls. It does not require a lot of investment and just needs restricted access to confidential files and applications in accordance with the job roles. For this it’s imperative that only employees who are relevant to a particular information can access it in order to complete their job. Once they don’t need that information anymore, revoke their access. Moreover, it is best not to give unlimited access to someone because of their seniority level in the organization. Also revoke email addresses and logins of an employee as soon as they leave your organization or change the department.

1. **Follow Best Password Practices**

“123456” has consecutively remained to be the most common password over the years. Though it seems like an untrivial measure, it’s often the weakest link to your sensitive information. Teach your employees to follow best practices such as how to keep strong passwords, keeping a different password every time and preferably using a password manager.

1. **Use Multi-Factor Authentication**

Multi-factor authentication is now commonly used by banks, social media accounts, ecommerce stores, or any business involved in [online transactions](http://www.cardzgroup.com/SmartTokenBands.html). It helps to add another security layer besides password to user accounts. Thus, any cybercriminal cannot access an account even after entering the correct password unless authenticated with a second or third factor. If your business involves creation of customer accounts, it’s preferable to enable multi-factor authentication to keep your data secure.

1. **Consider Remote Work Risks**

The pandemic has changed the way we work. Since remote work has now become a norm, it is now not possible to ignore the security risks associated with remote working. Though it’s convenient, it also has posed new challenges and threats. With more entry points and personal devices being used to perform jobs, cybercriminals have now more room for exploitation. Unsecured WiFi and personal devices can cause potential data breach, especially with no way to check and ensure that employees are not using these mediums.

Hence, the best way for a small business to tackle this is to devise a remote work policy that employees should strictly adhere to. It must state best practices including how employees should use their personal devices and install security patches regularly.

1. **Conduct Regular Employee Trainings**

Even with all the policies in place, employees tend to forget.

Hence, it’s important to conduct trainings at least twice a year for reinforcement of security concepts. Moreover, it is a plus if employees practice actual simulations and go through security breach drills to get a better idea of how to respond in real situations.

1. **Use Security Tools**

Along with cloud backup and password manager, invest in security software and tools such as anti-malware and firewalls. Even after receiving trainings, it is human nature to forget easily and make mistakes. Some employees will still get carried away and click malicious links in phishing emails. Anti-malware helps regularly scan for malware in your system and firewall creates a barrier between the attackers and your network.

1. **Keep Confidential Information Encrypted**

Enable your network encryption for ensuring secure transfer of your data online without interception threats with man-in-the-middle attacks.

Besides all these security measures, make cybersecurity a preference for your workplace. All these security measures do not require heavy investments, and you can easily implement them as a regular part of your workplace. Not only will it make your workplace more secure, it’ll also significantly improve your customer loyalty and business reputation.